AMENDMENT OF CONDITIONALLY ALLOWABLE CLAIM 38

Claim 38 has been rewritten in independent form, incorporating all the limitations of the base claim (Claim 1), as it stood prior to this amendment D. Claim 38 was directly dependent on Claim 1, with no intervening claims.

Claims 39-41 depend on Claim 38.

Applicant respectfully requests allowance of Claims 38-41.

AMENDMENT OF CLAIM 18 TO CORRECT A TYPOGRAPHICAL ERROR

Claim 18 has been amended to insert the word "field", unintentionally omitted from the original application. This clarifies that the multiplication referred to is a field multiplication, not a point multiplication.

REJECTION OF CLAIMS 1-37 AND 42-59 UNDER 35 U.S.C. 103(A)

AS UNPATENTABLE OVER VANSTONE IN VIEW OF KOYAMA

Claims 1-37 and 42-59 stand rejected under 35 U.S.C. 103(a) as unpatentable over Vanstone (Vanstone et al., US Patent 6,141,420) in view of Koyama (Koyama et al., Elliptic Curve

Cryptosystems and Their Applications, reference U).

The applicant has argued in a previous reply that the combination of Vanstone and Koyama is nonobvious because they don't and can't work together. Examiner argues that the test for obviousness is what the combined teachings of the references would have suggested to those of ordinary skill in the art.

Applicant makes two points:

1) As amended, the independent Claims 1, 26, and 29 include elements not present in either Koyama or Vanstone. The amended claims require five occurrences of point fractioning in the point modification method, and that the inputs of each fractioning (except the first) are dependent on the outputs of the previous fractioning. Koyama's paper uses one point halving in each of two independent elliptic curves, and those halvings don't affect each other. In the amended claims, chaining together the fractionings is a new element, and five fractionings is another new element. Neither of these elements appears in Koyama or Vanstone.

2) Applicant wishes to offer further evidence of the nonobviousness of the combination of Vanstone with Koyama.

Koyama and Vanstone published a joint paper that includes a condensed version of the Koyama reference U. [New Public-Key

Schemes Based on Elliptic Curves over the Ring Zn, Kenji Koyama, Ueli M. Maurer, Tatsuaki Okamoto, and Scott Vanstone, Abstracts of Crypto '91, pp 6.1-7, Santa Barbara CA, August 11-15, 1991. A copy is enclosed with this communication].

The joint paper includes the point halving algorithm from Koyama reference U. Since Vanstone was an author of this short paper, we may reasonably infer that he was aware of Koyama's use of point halving. And yet we find no mention of point halving in the Vanstone patent. The purpose described in Vanstone's patent, "to make elliptic curve cryptography efficient, practical, and viable" [column 5, lines 3-4] would be much better served if he used point halving as part of his point multiplication method. [Point halving avoids a bunch of finite field inversions (reciprocals), which are a major cost in elliptic curve calculations.]

Moreover, all of the elements for doing the required finite field arithmetic for point halving are present in Vanstone. The only thing missing is the control structure to implement the point halving formula, which is very similar to the control structure for the standard "double and add" method that Vanstone describes. Point halving in either hardware or software is substantially faster than doubling, and has equivalent functionality. As an inventor and patent applicant, Vanstone described the best methods he knew of to practice his invention. There's no reason he should neglect to mention point halving, if he knew of its advantages.

Two books have been written about implementing elliptic curve cryptography, with detailed attention to point multiplication in GF[2^K] fields and various point representations. They contain much of the same background material on elliptic curves as the Vanstone patent. [Vanstone also contains other information such as hardware design.] These books are

Elliptic Curve Public Key Cryptosystems, Alfred J. Menezes, Kluwer, 1993,

and

Implementing Elliptic Curve Cryptography, Michael Rosing, Manning Publications, 1999.

Neither book so much as mentions point halving. And yet point halving is a big improvement to the methods outlined in these books. Menezes should be aware of the Koyama-Maurer-Okamoto-Vanstone paper: he has collaborated with Vanstone since 1990 -- they have several joint papers -- and his book references the Koyama-Maurer-Okamoto-Vanstone paper and incorporates some material from the paper (but not point halving). Some of Menezes' recent papers do discuss point halving as a way to make elliptic curve operations more efficient.

Rosing's book was published eight years after the K-M-O-V paper, and he had ample time to research his subject.

Applicant submits that three persons skilled in the art of elliptic curve cryptography have failed to notice the advantages of combining point halving, as suggested by Koyama, with the background material for efficient elliptic curve cryptography as sketched in the Vanstone patent, because it is not obvious except in hindsight.

To see the utility of point halving for efficient elliptic curve cryptography, the practitioner skilled in the art must make four insights:

(a) That half-points exist.
Koyama supplies this.

(b) That halving is functionally as useful as doubling.
This is not a profound insight, but applicant has not seen it in the elliptic curve literature before 1999.

(c) That halving can be cheap, even cheaper than doubling.
This is the great barrier: Koyama's halving algorithm includes roughly a hundred point doubling steps, and half as many point additions. This makes it an expensive operation, on a level with a typical public key operation such as a modular exponentiation. Such operations are costly: They are things a user does once or twice in achieving a high-value goal like establishing a computer connection or signing a document. These are things where a user could say "it's worth waiting a second or two for this". Such operations are

not thought of as common repetitive ingredients to be used many times, as low level steps in a larger operation. It's like the difference between eating a bite of food and going to the store for groceries. Since Koyama includes a hundred doublings to accomplish one halving, his article teaches away from the idea that halving can be a cheap substitute for doubling.

(d) The detailed formula for halving.
That a cheap formula exists is not obvious. If someone knows what he's looking for, he can find it.

Applicant believes he was the first person to make this combination of insights a, b, c, and d.

For these reasons, applicant submits that the combination of the teachings of Koyama and Vanstone is not obvious, and respectfully requests withdrawal of this grounds for objection to Claims 1, 26, 29, and 59.

REJECTION OF CLAIM 59

Paragraph 10 of the Office Action, in rejecting Claim 59, asserts "Koyama teaches an Elliptic curve point modification algorithm comprising one or more ambiguous point triplication steps, where the ambiguity is resolved by determining if a

point is twice halvable" and cites Koyama, pages 52-53, section 2.3 "Halving algorithm".

Applicant can find no mention of triplication in Koyama. Ambiguity is mentioned on page 52, right column, Note (b), but this refers to an ambiguity in decoding a message, which is unrelated to the idea of ambiguous point triplication. Moreover, Koyama gives no method for resolving the ambiguity. Furthermore, Koyama refer to points that can be halved once, dividing the points of a curve into classes X and X′ based on whether they are doubles or not. But he never mentions testing if a point is twice halvable. He also makes no use of halvability for resolving ambiguity.

For these reasons, applicant submits that Claim 59 is not taught by Koyama, and respectfully requests the withdrawal of this ground for rejection of Claim 59.

REJECTION OF CLAIMS 36 AND 37

Paragraph 19 of the Office Action rejects Claim 36, wherein the elliptic curve is over a finite field which is represented by a field polynomial of low hamming weight. Vanstone, column 13, lines 60-62 is cited as teaching a field polynomial of low hamming weight.

In fact, Vanstone, column 13, lines 60-62 is not talking about a field polynomial. Vanstone is discussing the choice of the "seed key K". K is a number, used as the point multiplier in his encryption scheme. The number of 1 bits in the binary representation of K is the Hamming weight. Each 1 bit will require a point addition step (as explained in the middle of column 13). Vanstone suggests choosing K to be a number with a small Hamming weight. But K has nothing to do with the field polynomial. He has earlier used the notation P(X) [column 6, line 39-40] for the field polynomial.

The field polynomial should not be confused with the equation for the elliptic curve, [Vanstone, column 2, line 29-30], which often has only five or six terms, and contains at least two variables. A field polynomial has only one variable, and often appears alone, not as part of an equation.

Paragraph 20 of the Office Action rejects Claim 37, stating that Vanstone teaches "wherein the field polynomial is selected from a binomial, a trinomial, and a pentanomial (i.e. polynomials of degree 2, 3, and 5)." Column 8, lines 39-41, and column 6, lines 30-32 of Vanstone are cited.

This is mistaken. A binomial is a polynomial expression with two terms (combined with addition or subtraction), a trinomial is a polynomial with three terms, and a pentanomial is a polynomial with five terms. The degree of a polynomial is only loosely related to the number of terms.

Vanstone uses a trinomial, X^3 + X + 1, as his teaching example. (The degree of the teaching example is the same as the number of terms, 3, but this is coincidental. Another trinomial that could be used is X^5 + X^2 + 1, of degree 5.) Vanstone nowhere recommends that field polynomials of low hamming weight be used. He has selected a necessarily small example for his explanation. But he later suggests (column 14, line 20) the working field 2^155, which will have a field polynomial beginning with X^155, and likely containing many more terms. Vanstone is silent on the exact polynomial, but a typical field polynomial of that degree will have half of its possible coefficients being non-zero, or about 77 terms. This is not low hamming weight, and certainly not a binomial, trinomial, or pentanomial.

For these reasons, applicant submits that Claims 36 and 37 are not taught by Vanstone, and respectfully requests the withdrawal of this ground for rejection of Claims 36 and 37.

REJECTION OF CLAIM 55

Paragraph 21 of the Office Action rejects Claim 55, citing Vanstone, columns 20-21, Claims 32, 39, and 40. Claim 55 of the present application includes the concept "reducing the required storage of an efficient algorithm". Vanstone Claims 32, 39, and 40 say nothing about storage.

For this reason, applicant submits that Claim 55 is not taught by Vanstone, and respectfully requests the withdrawal of this ground for rejection of Claim 55.

REJECTION OF CLAIMS 47, 48, AND 51

Paragraph 27 of the Office Action rejects Claims 47 (chained point fractioning), 48 (omitting computation of some point coordinates) and 51 (addition-subtraction chain intermixed with point fractioning). The supporting citation is Vanstone, column 4, lines 7-25. But in fact, lines 7-25 describe the formula for addition of elliptic curve points. There is no mention of point fractioning at all. The formulas in lines 7-25 do describe fractions, but the numerators and denominators in these fractions are field elements, not elliptic curve points.

Vanstone doesn't appear to discuss subtraction of elliptic curve points, nor does he mention addition-subtraction chains. Vanstone doesn't discuss omitting the computation of some of the coordinates of an elliptic curve point. Vanstone doesn't discuss point fractioning, or the intermixing of point fractioning with an addition-subtraction chain.

For these reasons, applicant submits that Claims 47, 48, and 51 are not taught by Vanstone, and respectfully requests the withdrawal of this ground for rejection of Claims 47, 48, and 51.

REJECTION OF CLAIMS 56-58

Paragraph 29 of the Office Action rejects Claims 56-58, citing Vanstone, column 15, lines 51-65 and column 16, lines 1-20. Claim 56 requires "at least three changes of representation", but Vanstone is silent on the required number of changes. The minimum number of changes implied by his discussion is only two, from affine (X,Y) form to projective form (X,Y,Z) and back to affine.

Vanstone does not discuss XR representation (Claim 57) or switching between XY and XR representations (Claim 58).

For these reasons, applicant submits that Claims 56-58 are not taught by Vanstone, and respectfully requests the withdrawal of this ground for rejection of Claims 56-58.

REJECTION OF CLAIMS 7 AND 32

Paragraph 30 of the Office Action rejects Claims 7 and 32, citing several sections from Vanstone and Koyama. Claims 7 and 32 both include "wherein point multiplying is selected from integral multiplication, imaginary multiplication, and complex multiplication". Neither Vanstone nor Koyama mentions complex multiplication.

For this reason, applicant submits that Claims 7 and 32 are not taught by Vanstone together with Koyama, and respectfully requests the withdrawal of this ground for rejection of Claims 7 and 32.

REJECTION OF CLAIMS 18-20, 23, AND 24

Paragraph 33 of the Office Action rejects Claims 18-20, 23, and 24, citing Koyama and Vanstone.

Claim 18, as amended, emphasizes that point halving is to be done using "a single field multiplication per halving operation". Koyama's method for point halving requires a couple of hundred field multiplications: Each point doubling or point addition takes a couple of field multiplications, and Koyama needs more than a hundred point doubling (or

addition) steps to compute a single point halving step. Koyama requires operations modulo prime and composite numbers of size at least a couple of hundred bits, big enough that the composite numbers are difficult to factor. His halving algorithm requires that curve points be multiplied by numbers of similar size, and that requires a couple of hundred point doublings and additions.

Claim 19 requires "completing halving using no more than two field multiplications". Koyama requires hundreds of field multiplications for each halving step.

Claim 20 is about "negative halving". Neither Koyama nor Vanstone discusses negative halving.

Claim 23 requires "reliance on a bit mask of coordinates" to test whether a point is in a subgroup. Neither Vanstone nor Koyama mentions using a bit mask for testing subgroup membership.

Claim 24 requires "testing whether a halving procedure can be executed an arbitrary number of times selected by a user". Neither Koyama nor Vanstone mentions an arbitrary number of halvings.

For these reasons, applicant submits that Claims 18-20, 23, and 24 are not taught by Vanstone together with Koyama, and respectfully requests the withdrawal of this ground for rejection of Claims 18-20, 23, and 24.

CONCLUSION

By this paper, Claims 1, 26, and 29 have been amended to more fully distinguish the invention. Claim 18 has been amended to correct a typographical error. Claim 38 has been rewritten as an independent claim per the Examiner's suggestion. Claims 2-25, 27-28, 30-37, and 39-58 are dependent on Claims 1, 26, 29, and 38. Claim 59 is already distinguished over the cited art.

Applicant respectfully requests reconsideration of Claims 1-59 as amended. For reasons set forth above, Claims 1-59 are believed to be in condition for immediate allowance, and Applicant so requests.

In the event the Examiner finds any remaining impediment to the prompt allowance of any of these claims, which could be clarified in a telephone conference, the Examiner is respectfully urged to initiate the same with the undersigned.

DATED this 7th day of September, 2006.

Respectfully submitted,

Richard Schroeppel, Applicant
500 S. Maple Drive
Woodland Hills, Utah 84653
Telephone: 801-423-7998
Date: September 7, 2006